

## WEST Search History

[Hide Items](#) | [Restore](#) | [Clear](#) | [Cancel](#)

DATE: Friday, May 20, 2005

<u>Hide?</u>	<u>Set Name</u>	<u>Query</u>	<u>Hit Count</u>
		<i>DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR</i>	
<input type="checkbox"/>	L20	(feedback adj shift adj register\$1) near10( randomiz\$5 or permutat\$5) near10 (multiple or plurality) near10 stages	1
<input type="checkbox"/>	L19	L17 and (multiple or plurality) near3 register\$1 near3 (randomiz\$4 or permutat\$5)	4
<input type="checkbox"/>	L18	L17 and (multiple or plurality) near3 register\$1	139
<input type="checkbox"/>	L17	L15 and (feedback adj shift register)	800
<input type="checkbox"/>	L16	L15 and feedback adj shift register	747272
<input type="checkbox"/>	L15	380/44,46,47,262,265,268.ccls.	1560
<input type="checkbox"/>	L14	1999	24
<input type="checkbox"/>	L13	L12 and (randomiz\$4 or permutat\$4)	43
<input type="checkbox"/>	L12	(feedback adj shift adj register) near10 (plurality or multiple) near10 register\$1 and (dynamic or realtime or real adj time)	163
<input type="checkbox"/>	L11	(feedback adj shift adj register) near10 (plurality or multiple) near10 register\$1	482
<input type="checkbox"/>	L10	(feedback adj shift adj register) near10 (plurality or multiple) near10 dynamic	1
<input type="checkbox"/>	L9	feedback adj shift adj register	4022
<input type="checkbox"/>	L8	(randomiz\$5 or permutat\$4) with (plurality or multiple) with dynamic\$3 near10 shift adj registers	0
<input type="checkbox"/>	L7	(randomiz\$5 or permutat\$4) with (plurality or multiple) with shift adj registers	39
<input type="checkbox"/>	L6	L5 and (randomiz\$5 or permutat\$4) with (plurality or multiple) with shift adj registers	0
<input type="checkbox"/>	L5	L4 or l3 or l2 or l1	12
<input type="checkbox"/>	L4	(6763363 5727063 5515307).pn.	6
<input type="checkbox"/>	L3	20020006195.pn.	2
<input type="checkbox"/>	L2	20030206634.pn.	2
<input type="checkbox"/>	L1	20020015493.pn.	2

END OF SEARCH HISTORY

File 8:EI Compendex(R) 1970-2005/May W3  
 (c) 2005 Elsevier Eng. Info. Inc.  
 File 35:Dissertation Abs Online 1861-2005/Apr  
 (c) 2005 ProQuest Info&Learning  
 File 65:Inside Conferences 1993-2005/May W3  
 (c) 2005 BLDSC all rts. reserv.  
 File 2:INSPEC 1969-2005/May W3  
 (c) 2005 Institution of Electrical Engineers  
 File 94:JICST-EPlus 1985-2005/Apr W1  
 (c) 2005 Japan Science and Tech Corp(JST)  
 File 6:NTIS 1964-2005/May W2  
 (c) 2005 NTIS, Intl Cpyrgh All Rights Res  
 File 144:Pascal 1973-2005/May W3  
 (c) 2005 INIST/CNRS  
 File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec  
 (c) 1998 Inst for Sci Info  
 File 34:SciSearch(R) Cited Ref Sci 1990-2005/May W3  
 (c) 2005 Inst for Sci Info  
 File 99:Wilson Appl. Sci & Tech Abs 1983-2005/Apr  
 (c) 2005 The HW Wilson Co.  
 File 266:FEDRIP 2005/Jan  
 Comp & dist by NTIS, Intl Copyright All Rights Res  
 File 95:TEME-Technology & Management 1989-2005/Apr W2  
 (c) 2005 FIZ TECHNIK  
 File 62:SPIN(R) 1975-2005/Mar W1  
 (c) 2005 American Institute of Physics  
 File 239:Mathsci 1940-2005/Jun  
 (c) 2005 American Mathematical Society

Set	Items	Description
S1	8277	(FEEDBACK(N)SHIFT) ()REGISTER? ? OR FSR OR SFR OR LFSR OR L-SFR OR MFSR OR MSFR
S2	63	S1(5N) (DYNAMIC? OR REALTIME OR REAL()TIME OR ONDEMAND OR ON()DEMAND OR VIRTUAL?)
S3	0	(MORE() (THEN OR THAN) ()ONE) (5W)S2
S4	12	(MULTIPLE OR MULTIPLICITY OR MULTI OR SEVERAL OR MANY OR PLURAL? OR DUAL? OR VARIOUS OR NUMEROUS OR ASSORTMENT OR ADDITIONAL OR AUXILIARY OR ASSORTED OR SERIES OR ARRAY OR REDUNDANT OR SECOND? OR 2ND OR TWO OR PAIR? ? OR THREE OR 3 OR FOUR OR 4) (5N)S2
S5	32	(STATIC? OR FIXED OR PERMANENT?) (5N)S1
S6	62409	PERMUT?
S7	1467253	RANDOM? OR PSEUDORANDOM?
S8	2339	(KEYSTREAM OR KEY()STREAM) (3N)GENERAT? OR RNG OR PRNG
S9	0	S4 AND S5 AND S6
S10	0	S4 AND S5
S11	4	S2 AND S5
S12	3	RD (unique items)
S13	2307	DYNAMIC()FEEDBACK
S14	652	STATIC()FEEDBACK
S15	0	SHIFT()REGISTER? ? AND S13 AND S14
S16	1	SHIFT()REGISTER? ? AND S13:S14

12/5/1 (Item 1 from file: 8)  
DIALOG(R)File 8:EI Compendex(R)  
(c) 2005 Elsevier Eng. Info. Inc. All rts. reserv.

05996422 E.I. No: EIP02046840680  
Title: Test vector encoding using partial LFSR reseeding  
Author: Krishna, C.V.; Jas, Abhijit; Touba, Nur A.  
Corporate Source: Computer Engineering Research Center Dept. of Elec. and  
Computer Eng. University of Texas, Austin, TX 78712-1084, United States  
Conference Title: International Test Conference 2001 Proceedings  
Conference Location: Baltimore, MD, United States Conference Date:  
20011030-20011101  
Sponsor: IEEE Comp. Soc. Test Technology Technical Council; IEEE  
Philadelphia Section  
E.I. Conference No.: 58973  
Source: IEEE International Test Conference (TC) 2001. p 885-893 (IEEE cat  
n 01CH37260)  
Publication Year: 2001  
CODEN: PITCFN ISSN: 1089-3539  
Language: English  
Document Type: CA; (Conference Article) Treatment: T; (Theoretical); X;  
(Experimental)

Journal Announcement: 0202W1  
Abstract: A new form of LFSR reseeding that provides higher encoding  
efficiency and hence greater reduction in test data storage requirements is  
described. Previous forms of LFSR reseeding have been static (i.e.,  
test generation is stopped and the seed is loaded at one time) and have  
required full reseeding (i.e.,  $n=r$  bits are used for an  $r$ -bit LFSR). The  
new form of LFSR reseeding proposed here is dynamic (i.e., the seed is  
incrementally modified while test generation proceeds) and allows partial  
reseeding (i.e.  $n$  less than  $r$  bits can be used). Full static forms of  
LFSR reseeding are shown to be a special case of the new partial dynamic  
form of LFSR reseeding. In addition to providing better encoding  
efficiency, partial dynamic LFSR reseeding has a simpler hardware  
implementation than previous schemes based on multiple-polynomial LFSRs,  
and can generate each test vector in fewer clock cycles. Experimental  
results demonstrate the advantages of the new partial dynamic LFSR  
reseeding approach. 14 Refs.

Descriptors: \*Integrated circuit layout; Data storage equipment; Timing  
circuits; Encoding (symbols); Vectors; Polynomials

Identifiers: Clock cycles; Automatic test equipments (ATE)  
Classification Codes:  
714.2 (Semiconductor Devices & Integrated Circuits); 722.1 (Data  
Storage, Equipment & Techniques); 713.4 (Pulse Circuits); 723.2 (Data  
Processing); 921.1 (Algebra)  
714 (Electronic Components & Tubes); 722 (Computer Hardware); 713  
(Electronic Circuits); 723 (Computer Software, Data Handling &  
Applications); 921 (Applied Mathematics)  
71 (ELECTRONICS & COMMUNICATION ENGINEERING); 72 (COMPUTERS & DATA  
PROCESSING); 92 (ENGINEERING MATHEMATICS)

12/5/2 (Item 1 from file: 2)  
DIALOG(R)File 2:INSPEC  
(c) 2005 Institution of Electrical Engineers. All rts. reserv.

8248659 INSPEC Abstract Number: B2005-02-1265A-073, C2005-03-7410D-007  
Title: Achieving high encoding efficiency with partial dynamic LFSR  
reseeding  
Author(s): Krishna, C.V.; Jas, A.; Touba, N.A.  
Author Affiliation: Dept. of Electr. & Comput. Eng., Texas Univ., Austin,  
TX, USA  
Journal: ACM Transactions on Design Automation of Electronic Systems  
vol.9, no.4 p.500-16

Publisher: ACM,

Publication Date: Oct. 2004 Country of Publication: USA

CODEN: ATASFO ISSN: 1084-4309

SICI: 1084-4309(200410)9:4L.500:AHEE;1-Z

Material Identity Number: F110-2004-004

U.S. Copyright Clearance Center Code: 1084-4309/04/1000-0500\$5.00

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P)

Abstract: Previous forms of LFSR reseeding have been **static** (i.e., test application is stopped while each seed is loaded) and have required full reseeding (i.e., the length of the seed is equal to the length of the LFSR). A form of LFSR reseeding is described here that is **dynamic** (i.e., the seed is incrementally modified while test application proceeds) and allows partial reseeding (i.e. length of the seed is less than that of the LFSR). In addition to providing better encoding efficiency, partial **dynamic** LFSR reseeding has a simpler hardware implementation than previous schemes based on multiple-polynomial LFSRs. (22 Refs)

Subfile: B C

Descriptors: built-in self test; encoding; integrated circuit testing; logic testing; shift registers

Identifiers: partial **dynamic** LFSR reseeding; linear feedback shift register; multiple-polynomial LFSR; built-in self-test

Class Codes: B1265A (Digital circuit design, modelling and testing); B7210A (Automatic test systems); B1265B (Logic circuits); C7410D (Electronic engineering computing); C5210 (Logic design methods); C5120 (Logic and switching circuits)

Copyright 2005, IEE

(Ein Generator von Mehrfachfolgen auf der Basis von invertierten, nichtlinearen autonomen Maschinen)

Chung-Len Lee; Meng-Lieh Sheu

Dept. of Electron. Eng., Nat. Chiao Tung Univ., Hsinchu, Taiwan

IEEE Transactions on Computers, v45, n9, pp1079-1083, 1996

Document type: journal article Language: English

Record type: Abstract

ISSN: 0018-9340

ABSTRACT:

A new multiple-sequence generator scheme to generate a set of deterministic ordered sequence of patterns followed by random patterns is presented in this paper. This scheme is based on an inverted nonlinear autonomous machine which utilizes a two-dimension-like LFSR with nonlinear inverters. A systematic procedure is also presented to obtain the autonomous machine which is more regular in the structure and utilizes less hardware. The generated deterministic sequence of patterns, which may have ordered and repeated patterns, and the random patterns are applicable to sequential circuit testing.

DESCRIPTORS: SEQUENTIAL CIRCUITS; SHIFT REGISTERS; CIRCUIT LOGIC; GATES-- CIRCUITS; ABSTRACT AUTOMATON; AUTOMATA THEORY; INVERTERS--LOGIC; RANDOM NUMBER; STOCHASTICS; RANDOM PROCESS; LOGIC TESTING

IDENTIFIERS: BINARY SEQUENCES; NONLINEAR AUTONOMOUS MACHINES; MULTIPLE SEQUENCE GENERATOR; INVERTED NONLINEAR AUTONOMOUS MACHINE; LFSR; NONLINEAR INVERTERS; DETERMINISTIC ORDERED SEQUENCE GENERATION; RANDOM PATTERN GENERATION; AUTONOMOUS MACHINE; LINEAR FEEDBACK SHIFT REGISTER; SEQUENTIAL CIRCUIT TESTING; AUTONOMER AUTOMAT; Mehrfachsequenzgenerator; autonomer Automat; Logiktest

13/3,K/1 (Item 1 from file: 348)  
DIALOG(R) File 348:EUROPEAN PATENTS  
(c) 2005 European Patent Office. All rts. reserv.

01367746

Method and apparatus for resolving data references in generated code

Gerat zur Auflösung von Datenreferenzen in erzeugtem Kode

Appareil pour resoudre des references de donnees dans un code genere

PATENT ASSIGNEE:

SUN MICROSYSTEMS, INC., (1392730), 2550 Garcia Avenue, Mountain View, CA  
94043, (US), (Applicant designated States: all)

INVENTOR:

Gosling, James, 363 Ridge Road, Woodside, California 94062, (US)

LEGAL REPRESENTATIVE:

Wombwell, Francis et al (46021), Potts, Kerr & Co. 15, Hamilton Square,  
Birkenhead Merseyside L41 6BR, (GB)

PATENT (CC, No, Kind, Date): EP 1164478 A2 011219 (Basic)

APPLICATION (CC, No, Date): EP 2001117182 931014;

PRIORITY (CC, No, Date): US 994655 921222

DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC;  
NL; PT; SE

RELATED PARENT NUMBER(S) - PN (AN):

EP 989488 (EP 99113405)

EP 604002 (EP 93308205)

INTERNATIONAL PATENT CLASS: G06F-009/45

ABSTRACT WORD COUNT: 200

NOTE:

Figure number on first page: 4

LANGUAGE (Publication,Procedural,Application): English; English; English  
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200151	2247
SPEC A	(English)	200151	2491
Total word count - document A			4738
Total word count - document B			0
Total word count - documents A + B			4738

...SPECIFICATION the ADD and the IF interpretation routines, 74 and 76, and  
two data reference interpretation routines, a static field reference  
routine ( SFR ) and a dynamic field reference routine (DFR), 78 and 80.  
The main interpreter routine 72 receives the byte codes 82...

13/3,K/2 (Item 2 from file: 348)  
DIALOG(R) File 348:EUROPEAN PATENTS  
(c) 2005 European Patent Office. All rts. reserv.

01131707

Method and apparatus for resolving data references in generated code

Verfahren und Gerat zur Auflösung von Datenreferenzen in erzeugtem Kode

Methode et appareil pour resoudre des references de donnees dans un code  
genere

PATENT ASSIGNEE:

SUN MICROSYSTEMS, INC., (1392730), 2550 Garcia Avenue, Mountain View, CA  
94043, (US), (Applicant designated States: all)

INVENTOR:

Gosling, James C/o Sun Microsystems, Inc. MTV29-236, 901 San Antonio Road,  
Palo Alto California 94303, (US)

LEGAL REPRESENTATIVE:

Wombwell, Francis (46022), Potts, Kerr & Co. 15, Hamilton Square,  
Birkenhead Merseyside CH41 6BR, (GB)

PATENT (CC, No, Kind, Date): EP 989488 A2 000329 (Basic)

APPLICATION (CC, No, Date): EP 99113405 931014;

PRIORITY (CC, No, Date): US 994655 921222

DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC;

NL; PT; SE

RELATED PARENT NUMBER(S) - PN (AN) :

EP 604002 (EP 93308205)

RELATED DIVISIONAL NUMBER(S) - PN (AN) :

(EP 2001117182)

INTERNATIONAL PATENT CLASS: G06F-009/45

ABSTRACT WORD COUNT: 200

NOTE:

Figure number on first page: 2

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200013	2731
SPEC A	(English)	200013	2521
Total word count - document A			5252
Total word count - document B			0
Total word count - documents A + B			5252

...SPECIFICATION the ADD and the IF interpretation routines, 74 and 76, and two data reference interpretation routines, a static field reference routine ( SFR ) and a dynamic field reference routine (DFR), 78 and 80. The main interpreter routine 72 receives the byte codes 82...

13/3, K/3 (Item 3 from file: 348)

DIALOG(R) File 348:EUROPEAN PATENTS

(c) 2005 European Patent Office. All rts. reserv.

00601862

Apparatus for resolving data references in generated code

Gerat zur Auflösung von Datenreferenzen in erzeugtem Kode

Appareil pour résoudre des références de données dans un code généré

PATENT ASSIGNEE:

SUN MICROSYSTEMS, INC., (1392730), 2550 Garcia Avenue, Mountain View, CA 94043, (US), (Proprietor designated states: all)

INVENTOR:

Gosling, James, P.O Box 620509, Woodside, California 94062, (US)

LEGAL REPRESENTATIVE:

Wombwell, Francis (46021), Potts, Kerr & Co. 15, Hamilton Square, Birkenhead Merseyside L41 6BR, (GB)

PATENT (CC, No, Kind, Date): EP 604002 A2 940629 (Basic)  
EP 604002 A3 950426  
EP 604002 B1 000517

APPLICATION (CC, No, Date): EP 93308205 931014;

PRIORITY (CC, No, Date): US 994655 921222

DESIGNATED STATES: DE; FR; GB; NL

RELATED DIVISIONAL NUMBER(S) - PN (AN) :

EP 989488 (EP 99113405)

INTERNATIONAL PATENT CLASS: G06F-009/45; G06F-009/445

ABSTRACT WORD COUNT: 206

NOTE:

Figure number on first page: 2

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200020	284
CLAIMS B	(German)	200020	263
CLAIMS B	(French)	200020	312
SPEC B	(English)	200020	2463
Total word count - document A			0
Total word count - document B			3322
Total word count - documents A + B			3322

...SPECIFICATION the ADD and the IF interpretation routines, 74 and 76, and two data reference interpretation routines, a static field reference routine ( SFR ) and a dynamic field reference routine ( DFR ), 78 and 80. The main interpreter routine 72 receives the byte codes 82...

13/3, K/4 (Item 4. from file: 348)  
DIALOG(R) File 348:EUROPEAN PATENTS  
(c) 2005 European Patent Office. All rts. reserv.

00480365  
Block-cipher cryptographic device based upon a pseudorandom nonlinear sequence generator.

Einrichtung zur Blockchiffrierung, welche auf der Anwendung eines nichtlinearen Pseudozufallsfolgengenerators beruht.

Dispositif cryptographique de chiffrage par bloc base sur un generateur de sequence pseudoaleatoire non-lineaire.

PATENT ASSIGNEE:

GENERAL INSTRUMENT CORPORATION OF DELAWARE, (1403171), 2200 Byberry Road, Hatboro, Pennsylvania 19040, (US), (applicant designated states:  
AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;LU;NL;SE)

INVENTOR:

Moroney, Paul, 1249 Avocet Court, Cardiff-By-The-Sea, California 92007, (US)

Bennett, Christopher John, 4280 Vista Street, San Diego, California 92116, (US)

Kindred, Daniel Ray, 3405 Texas Street, San Diego, California 92104, (US)

LEGAL REPRESENTATIVE:

Blatchford, William Michael et al (48801), Withers & Rogers 4 Dyer's Buildings Holborn, London EC1N 2JT, (GB)

PATENT (CC, No, Kind, Date): EP 443752 A2 910828 (Basic)

EP 443752 A3 921021

EP 443752 B1 951108

APPLICATION (CC, No, Date): EP 91300986 910206;

PRIORITY (CC, No, Date): US 482644 900221

DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IT; LI; LU; NL; SE

INTERNATIONAL PATENT CLASS: H04L-009/06;

ABSTRACT WORD COUNT: 299

LANGUAGE (Publication, Procedural, Application): English; English; English  
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	463
CLAIMS B	(English)	EPAB95	759
CLAIMS B	(German)	EPAB95	668
CLAIMS B	(French)	EPAB95	916
SPEC A	(English)	EPABF1	1969
SPEC B	(English)	EPAB95	2468
Total word count - document A			2432
Total word count - document B			4811
Total word count - documents A + B			7243

...SPECIFICATION Brown. The preferred embodiment of the DFAST keystream generator 32, as described in said patent, includes a dynamic (or nonlinear) feedback shift register and a static (or linear) feedback shift register for receiving input data. The most significant bytes of the N bytes 28 are received in the dynamic feedback shift register and the remaining bytes are received in the static feedback shift register of the DFAST keystream generator 32. The DFAST keystream generator 32 provides high speed pseudorandom nonlinear sequence...

...SPECIFICATION Brown. The preferred embodiment of the DFAST keystream generator 32, as described in said patent, includes a dynamic (or

nonlinear) feedback shift register and a static (or linear) feedback shift register for receiving input data. The most significant bytes of the N bytes 28 are received in the dynamic feedback shift register and the remaining bytes are received in the static feedback shift register of the DFAST keystream generator 32. The DFAST keystream generator 32 provides high speed pseudorandom nonlinear sequence...

13/3, K/5 (Item 5 from file: 348)

DIALOG(R) File 348:EUROPEAN PATENTS

(c) 2005 European Patent Office. All rts. reserv.

00364841

Dynamic feedback arrangement scrambling technique keystream generator.  
Dynamische Ruckkopplungsvorrichtung fur einen Verschleierungsschlüsselgenerat or.  
Dispositif de reaction dynamique pour generateur de sequence de cle d'un brouilleur.

PATENT ASSIGNEE:

GENERAL INSTRUMENT CORPORATION, (264771), 767 Fifth Avenue, New York New York 10153, (US), (applicant designated states:  
AT;BE;CH;DE;ES;FR;GB;GR;IT;LI;NL;SE)

INVENTOR:

Brown, David S., 147 Little Oaks Road, Encinitas California 92024, (US)

LEGAL REPRESENTATIVE:

Cookson, Barbara Elizabeth et al (50341), WITHERS & ROGERS 4 Dyer's Buildings Holborn, London EC1N 2JT, (GB)

PATENT (CC, No, Kind, Date): EP 342832 A2 891123 (Basic)  
EP 342832 A3 910529  
EP 342832 B1 940406

APPLICATION (CC, No, Date): EP 89304574 890505;

PRIORITY (CC, No, Date): US 194850 880517

DESIGNATED STATES: AT; BE; CH; DE; ES; FR; GB; GR; IT; LI; NL; SE

INTERNATIONAL PATENT CLASS: H04L-009/00;

ABSTRACT WORD COUNT: 232

LANGUAGE (Publication,Procedural,Application): English; English; English  
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS	B (English)	EPABF1	841
SPEC	B (English)	EPABF1	3983
Total word count - document	A		0
Total word count - document	B		4824
Total word count - documents	A + B		4824

...SPECIFICATION of a keystream generator according to the present invention.

Figure 2 is a block diagram of the dynamic feedback shift register structure included in the keystream generator of Figure 1.

Figure 3 is a block...

...1, a preferred embodiment of the keystream generator of the present invention includes a dynamic feedback shift register structure 10, a static feedback shift register structure 12, an input buffer 14, a plurality of ROMs 16, 17, 18, 19, 20, a plurality...  
...bits of the input data key are loaded in parallel from the input buffer 14 into the dynamic feedback shift register structure 10; and half of the bits of the input data signal are loaded in parallel from the input buffer 14 into the static feedback shift register structure 12.

Referring to Figure 2, the dynamic feedback shift register structure 10 includes "n" stages, with stage n being the input stage, stage 1 being the output...XOR gate 34 with the data bits shifted from

the LSB output stage (stage 1) of the **dynamic feedback shift register** structure 10 to provide on line 48 the data bit RG1 that is fed back to the...

...applied thereto.

In the preferred embodiment, each feedback shift register structure 10, 12 has 32 stages. The **static feedback shift register** structure 12 implements a primitive, irreducible polynomial of degree 32 to generate a maximal-length binary sequence...

File 347:JAPIO Nov 1976-2005/Jan (Updated 050506)

(c) 2005 JPO & JAPIO

File 350:Derwent WPIX 1963-2005/UD,UM &UP=200532

(c) 2005 Thomson Derwent

Set	Items	Description
S1	980	(FEEDBACK(N) SHIFT) () REGISTER? ? OR FSR OR SFR OR LFSR OR LSFR OR MFSR OR MSFR
S2	7	S1(5N) (DYNAMIC? OR REALTIME OR REAL() TIME OR ONDEMAND OR ON() DEMAND OR VIRTUAL?)
S3	0	(MORE() (THEN OR THAN) () ONE) (5W) S2
S4	0	(MULTIPLE OR MULTIPLICITY OR MULTI OR SEVERAL OR MANY OR PLURAL? OR DUAL? OR VARIOUS OR NUMEROUS OR ASSORTMENT OR ADDITIONAL OR AUXILIARY OR ASSORTED OR SERIES OR ARRAY OR REDUNDANT OR SECOND? OR 2ND OR TWO OR PAIR? ? OR THREE OR 3 OR FOUR OR 4) (5N) S2
S5	7	(STATIC? OR FIXED OR PERMANENT?) (5N) S1
S6	2367	PERMUT?
S7	118753	RANDOM? OR PSEUDORANDOM?
S8	183	(KEYSTREAM OR KEY() STREAM) (3N) GENERAT? OR RNG OR PRNG
S9	1	S2 AND S5
S10	1084	FEEDBACK(5N) (DYNAMIC? OR REALTIME OR REAL() TIME OR ONDEMAND OR ON() DEMAND OR VIRTUAL?)
S11	670	FEEDBACK(5N) (STATIC? OR FIXED OR PERMANENT?)
S12	15	S10 AND S11
S13	1	S12 AND SHIFT() REGISTER? ?
S14	1	S12 AND S6:S7
S15	2	S9 OR S13:S14

15/5/1 (Item 1 from file: 350)  
DIALOG(R)File 350:Derwent WPIX  
(c) 2005 Thomson Derwent. All rts. reserv.

013905707 \*\*Image available\*\*  
WPI Acc No: 2001-389920/200141  
XRPX Acc No: N01-286860

Cryptographic one way function generation apparatus for use in encrypting or decrypting binary data

Patent Assignee: GEN INSTR CORP (GENN )

Inventor: QIU X; SPRUNK E J

Number of Countries: 095 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200139417	A2	20010531	WO 2000US31539	A	20001117	200141 B
AU 200117705	A	20010604	AU 200117705	A	20001117	200153
EP 1232603	A2	20020821	EP 2000980446	A	20001117	200262
			WO 2000US31539	A	20001117	
KR 2002060237	A	20020716	KR 2002706549	A	20020522	200305
CN 1425230	A	20030618	CN 2000818544	A	20001117	200358
TW 548937	A	20030821	TW 2000124901	A	20001123	200409

Priority Applications (No Type Date): US 99167185 P 19991123

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200139417	A2	E	59	H04L-000/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR

IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200117705 A H04L-000/00 Based on patent WO 200139417

EP 1232603 A2 E H04L-009/26 Based on patent WO 200139417

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR

KR 2002060237 A H04L-009/26

CN 1425230 A H04L-009/26

TW 548937 A H04L-009/00

Abstract (Basic): WO 200139417 A2

NOVELTY - A non-linear key or keystream generation algorithm uses multiple feedback shift registers (120, 130). The feedback shift registers are constructed using an advanced mathematical construct called an extended Galois Fields GF(2<sup>m</sup>). The key or keystream (100) is generated as a non-linear function of the outputs (RGA, RGB, RGC) of the multiple feedback shift registers.

DETAILED DESCRIPTION - The shift registers may be a combination of static feedback shift registers and dynamic feedback shift registers (120, 130).

USE - For the generation of a cryptographic one way function (a key or keystream generator) for use in encrypting or decrypting binary data.

ADVANTAGE - Produces a cryptographically robust keystream.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of the apparatus.

Outputs (RGA, RGB, RGC)

Key or keystream (100)

Multiple feedback shift registers (120, 130)

pp; 59 DwgNo 3b/6

Title Terms: CRYPTOGRAPHIC; ONE; WAY; FUNCTION; GENERATE; APPARATUS; BINARY ; DATA

Derwent Class: T01; U21; W01

International Patent Class (Main): H04L-000/00; H04L-009/00; H04L-009/26

File Segment: EPI

15/5/2 (Item 2 from file: 350)  
DIALOG(R) File 350:Derwent WPIX  
(c) 2005 Thomson Derwent. All rts. reserv.

007654114 \*\*Image available\*\*

WPI Acc No: 1988-288046/198841

XRPX Acc No: N88-218603

Radio frequency tracking loop for spread spectrum system - has output signals of peak tracking circuits of both in-phase and quadrature channels applied to Costas loop multiplier

Patent Assignee: STC PLC (STTE )

Inventor: FORSYTH S M; ROLLEY R; WONG A C C

Number of Countries: 001 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
GB 2203303	A	19881012	GB 877599	A	19870331	198841 B
GB 2203303	B	19910213				199107

Priority Applications (No Type Date): GB 877599 A 19870331

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
GB 2203303	A		9		

Abstract (Basic): GB 2203303 A

A costas-loop carrier-recovery circuit includes digitisers (20,21), correlators (18,19) and a peak-tracking circuit (22) in each I & Q arm. The correlators produce a peak output which indicates a degree of correlation between the input pseudo-random code and a reference code. The peak tracker holds the values (23,24) which are multiplied together (16) to produce a static feedback control signal until such time as dynamic feedback is returned.

The feedback loop includes a filter (16a) to which the error voltage output of multiplier (16) is applied. The kind of loop filter selected depends upon the dynamic acquisition and tracking ability required for a given application. E.g. a proportional plus integral filter allows the loop to track phase and frequency steps in the carrier with no error in the steady-state and frequency ramps (Doppler shifts) with a constant steady-state error.

USE - For direct-sequence, binary-phase-coded, spread-spectrum system.

File 348:EUROPEAN PATENTS 1978-2005/May W03

(c) 2005 European Patent Office

File 349:PCT FULLTEXT 1979-2005/UB=20050519,UT=20050512

(c) 2005 WIPO/Univentio

Set	Items	Description
S1	3275	(FEEDBACK(N)SHIFT) ()REGISTER? ? OR FSR OR SFR OR LFSR OR LSFR OR MFSR OR MSFR
S2	33	S1(5N)(DYNAMIC? OR REALTIME OR REAL()TIME OR ONDEMAND OR ON()DEMAND OR VIRTUAL?)
S3	0	(MORE() (THEN OR THAN) ()ONE) (5W)S2
S4	8	(MULTIPLE OR MULTIPLICITY OR MULTI OR SEVERAL OR MANY OR PLURAL? OR DUAL? OR VARIOUS OR NUMEROUS OR ASSORTMENT OR ADDITIONAL OR AUXILIARY OR ASSORTED OR SERIES OR ARRAY OR REDUNDANT OR SECOND? OR 2ND OR TWO OR PAIR? ? OR THREE OR 3 OR FOUR OR 4) (5N)S2
S5	66	(STATIC? OR FIXED OR PERMANENT?) (5N)S1
S6	15153	PERMUT?
S7	218471	RANDOM? OR PSEUDORANDOM?
S8	5048	(KEYSTREAM OR KEY()STREAM) (3N)GENERAT? OR RNG OR PRNG
S9	1	S4(50N)S5(50N)S6
S10	1	S4(100N)S5(100N)S6
S11	1	S4(50N)S5
S12	6	S2(50N)S5
S13	6	S2(100N)S5
S14	3206	FEEDBACK(5N) (DYNAMIC? OR REALTIME OR REAL()TIME OR ONDEMAND OR ON()DEMAND OR VIRTUAL?)
S15	1042	FEEDBACK(5N) (STATIC? OR FIXED OR PERMANENT?)
S16	40	S14(50N)S15
S17	4	S14(50N)S15(50N) (SHIFT()REGISTER? ?)
S18	1	S17 NOT S13
S19	3	S14(50N)S15(50N)S6:S7
S20	53	(NONLINEAR OR (NON OR "NOT" OR T) (2W)LINEAR) (3W)S1
S21	955	LINEAR (3W)S1
S22	43	S20(50N)S21
S23	0	(MORE() (THEN OR THAN) ()ONE) (5W)S20
S24	7	(MULTIPLE OR MULTIPLICITY OR MULTI OR SEVERAL OR MANY OR PLURAL? OR DUAL? OR VARIOUS OR NUMEROUS OR ASSORTMENT OR ADDITIONAL OR AUXILIARY OR ASSORTED OR SERIES OR ARRAY OR REDUNDANT OR SECOND? OR 2ND OR TWO OR PAIR? ? OR THREE OR 3 OR FOUR OR 4) (5W)S20
S25	3	S24(50N)S21
S26	0	S24(50N)S5
S27	1	S21(50N)S4
S28	4	S25:S27
S29	8	S24 OR S28

File 8:Ei Compendex(R) 1970-2005/May W3  
     (c) 2005 Elsevier Eng. Info. Inc.  
 File 35:Dissertation Abs Online 1861-2005/Apr  
     (c) 2005 ProQuest Info&Learning  
 File 65:Inside Conferences 1993-2005/May W3  
     (c) 2005 BLDSC all rts. reserv.  
 File 2:INSPEC 1969-2005/May W3  
     (c) 2005 Institution of Electrical Engineers  
 File 94:JICST-EPlus 1985-2005/Apr W1  
     (c) 2005 Japan Science and Tech Corp(JST)  
 File 6:NTIS 1964-2005/May W2  
     (c) 2005 NTIS, Intl Cpyrgh All Rights Res  
 File 144:Pascal 1973-2005/May W3  
     (c) 2005 INIST/CNRS  
 File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec  
     (c) 1998 Inst for Sci Info  
 File 34:SciSearch(R) Cited Ref Sci 1990-2005/May W3  
     (c) 2005 Inst for Sci Info  
 File 99:Wilson Appl. Sci & Tech Abs 1983-2005/Apr  
     (c) 2005 The HW Wilson Co.  
 File 266:FEDRIP 2005/Jan  
     Comp & dist by NTIS, Intl Copyright All Rights Res  
 File 95:TEME-Technology & Management 1989-2005/Apr W2  
     (c) 2005 FIZ TECHNIK  
 File 62:SPIN(R) 1975-2005/Mar W1  
     (c) 2005 American Institute of Physics  
 File 239:Mathsci 1940-2005/Jun  
     (c) 2005 American Mathematical Society

Set	Items	Description
S1	8277	(FEEDBACK(N)SHIFT) ()REGISTER? ? OR FSR OR SFR OR LFSR OR L-SFR OR MFSR OR MSFR
S2	63	S1(5N) (DYNAMIC? OR REALTIME OR REAL()TIME OR ONDEMAND OR O-N()DEMAND OR VIRTUAL?)
S3	0	(MORE() (THEN OR THAN) ()ONE) (5W)S2
S4	12	(MULTIPLE OR MULTIPLICITY OR MULTI OR SEVERAL OR MANY OR PLURAL? OR DUAL? OR VARIOUS OR NUMEROUS OR ASSORTMENT OR ADDITIONAL OR AUXILIARY OR ASSORTED OR SERIES OR ARRAY OR REDUNDANT OR SECOND? OR 2ND OR TWO OR PAIR? ? OR THREE OR 3 OR FOUR OR 4) (5N)S2
S5	32	(STATIC? OR FIXED OR PERMANENT?) (5N)S1
S6	174	(NONLINEAR OR (NON OR "NOT" OR T) (2W)LINEAR) (3W)S1
S7	2769	LINEAR(3W)S1
S8	0	(MORE() (THEN OR THAN) ()ONE) (5W)S6
S9	8	(MULTIPLE OR MULTIPLICITY OR MULTI OR SEVERAL OR MANY OR PLURAL? OR DUAL? OR VARIOUS OR NUMEROUS OR ASSORTMENT OR ADDITIONAL OR AUXILIARY OR ASSORTED OR SERIES OR ARRAY OR REDUNDANT OR SECOND? OR 2ND OR TWO OR PAIR? ? OR THREE OR 3 OR FOUR OR 4) (5W)S6
S10	5	S9 AND (S7 OR S5)
S11	1	S7 AND S4
S12	6	S10:S11
S13	4	RD (unique items)

File 347:JAPIO Nov 1976-2005/Jan(Updated 050506)

(c) 2005 JPO & JAPIO

File 350:Derwent WPIX 1963-2005/UD,UM &UP=200532

(c) 2005 Thomson Derwent

Set	Items	Description
S1	980	(FEEDBACK(N)SHIFT) ()REGISTER? ? OR FSR OR SFR OR LFSR OR LSFR OR MFSR OR MSFR
S2	7	S1(5N) (DYNAMIC? OR REALTIME OR REAL()TIME OR ONDEMAND OR ON()DEMAND OR VIRTUAL?)
S3	0	(MORE() (THEN OR THAN) ()ONE) (5W)S2
S4	0	(MULTIPLE OR MULTIPLICITY OR MULTI OR SEVERAL OR MANY OR PLURAL? OR DUAL? OR VARIOUS OR NUMEROUS OR ASSORTMENT OR ADDITIONAL OR AUXILIARY OR ASSORTED OR SERIES OR ARRAY OR REDUNDANT OR SECOND? OR 2ND OR TWO OR PAIR? ? OR THREE OR 3 OR FOUR OR 4) (5N)S2
S5	7	(STATIC? OR FIXED OR PERMANENT?) (5N)S1
S6	18	(NONLINEAR OR (NON OR "NOT" OR T) (2W)LINEAR) (3W)S1
S7	403	LINEAR(3W)S1
S8	0	(MORE() (THEN OR THAN) ()ONE) (5W)S6
S9	5	(MULTIPLE OR MULTIPLICITY OR MULTI OR SEVERAL OR MANY OR PLURAL? OR DUAL? OR VARIOUS OR NUMEROUS OR ASSORTMENT OR ADDITIONAL OR AUXILIARY OR ASSORTED OR SERIES OR ARRAY OR REDUNDANT OR SECOND? OR 2ND OR TWO OR PAIR? ? OR THREE OR 3 OR FOUR OR 4) (5W)S6
S10	3	S9 AND (S7 OR S5)

10/5/1 (Item 1 from file: 347)  
DIALOG(R) File 347:JAPIO  
(c) 2005 JPO & JAPIO. All rts. reserv.

06434718 \*\*Image available\*\*  
PSEUDO RANDOM NUMBER GENERATOR

PUB. NO.: 2000-020284 [JP 2000020284 A]  
PUBLISHED: January 21, 2000 (20000121)  
INVENTOR(s): SUGIMOTO KOICHI  
APPLICANT(s): TOYO COMMUN EQUIP CO LTD  
APPL. NO.: 10-196639 [JP 98196639]  
FILED: June 26, 1998 (19980626)  
INTL CLASS: G06F-007/58

#### ABSTRACT

PROBLEM TO BE SOLVED: To provide a generator hardly presunable its initial value by using a Correlation Attack or the like by constituting the generator combining a linear feedback shift register and a non-linear feedback shift register.

SOLUTION: This generator has a linear feedback shift register 3 and non - linear feedback shift register 4 to be operated synchronously with the same clock input and a non-linear conversion function circuit 5 for outputting the pseudo random number of 1 bit by performing non-linear conversion to respective register values from the linear feedback shift register 3 and non - linear feedback shift register 4. In the generator, the respective register values of the linear feedback shift register 3 and non - linear feedback shift register 4 to be operated synchronously with the clock input are inputted to the non-linear conversion function circuit 5. The pseudo random number of 1 bit is outputted at the interval of one to several clocks.

COPYRIGHT: (C) 2000, JPO

10/5/2 (Item 1 from file: 350)  
DIALOG(R) File 350:Derwent WPIX  
(c) 2005 Thomson Derwent. All rts. reserv.

016892172 \*\*Image available\*\*  
WPI Acc No: 2005-216459/200523  
XRPX Acc No: N05-178964  
Pseudo-random number generator for e.g. chip card, has combination unit to combine outputs of non linear feedback shift registers to obtain combined signal comprising pseudo random number at output

Patent Assignee: INFINEON TECHNOLOGIES AG (INFN )

Inventor: DIRSCHERL G; GAMMEL B; GOETTFERT R; GOTTFERT R

Number of Countries: 003 Number of Patents: 003

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
FR 2859290	A1	20050304	FR 20049138	A	20040827	200523 B
DE 10339999	A1	20050407	DE 10339999	A	20030829	200524
US 20050097153	A1	20050505	US 2004925903	A	20040823	200531

Priority Applications (No Type Date): DE 10339999 A 20030829

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
FR 2859290	A1	48		G06F-007/58	
DE 10339999	A1			G06F-007/58	
US 20050097153	A1			G06F-001/02	

Abstract (Basic): FR 2859290 A1

NOVELTY - The generator has three non linear feedback

shift registers (101-103) with respective outputs (101a-103a). A combination unit (120) has a multiplier (120a) and adder (120b) to combine the outputs of the non linear feedback shift registers to obtain a combined signal comprising a pseudo random number at an output (122) of the combination unit.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) a method for generating a pseudo-random number

(b) a computer program having a program code to perform a method of generating a pseudo-random number.

USE - Used in an integrated circuit or chip card for generating a pseudo random number for a pay-television application and cellular telephone for cryptography.

ADVANTAGE - The generator is simple, flexible and reliable to generate a pseudo random number with high linear complexity and increased length of period of generation, therefore the random number containing the secret information cannot be localized by the cryptographic attacker.

DESCRIPTION OF DRAWING(S) - The drawing shows a pseudo random number generator.

Non linear feedback shift registers (101-103)

Register outputs (101a-103a)

Combination unit (120)

Multiplier (120a)

Adder (120b)

Combination unit output (122)

pp; 48 DwgNo 1/12

Title Terms: PSEUDO; RANDOM; NUMBER; GENERATOR; CHIP; CARD; COMBINATION; UNIT; COMBINATION; OUTPUT; NON; LINEAR; FEEDBACK; SHIFT; REGISTER; OBTAIN ; COMBINATION; SIGNAL; COMPRISE; PSEUDO; RANDOM; NUMBER; OUTPUT

Derwent Class: T01; T04; W01; W02

International Patent Class (Main): G06F-001/02; G06F-007/58

File Segment: EPI

10/5/3 (Item 2 from file: 350)

DIALOG(R) File 350:Derwent WPIX

(c) 2005 Thomson Derwent. All rts. reserv.

012993333 \*\*Image available\*\*

WPI Acc No: 2000-165185/200015

XRPX Acc No: N00-123683

Dummy random number generator for e.g. encryption communication apparatus - performs nonlinear conversion of outputs of linear and nonlinear feedback shift registers to output one-bit dummy random number for every one-number clock

Patent Assignee: TOYO COMMUNICATION EQUIP CO (TOCM )

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 2000020284	A	20000121	JP 98196639	A	1998062	200015 B

Priority Applications (No Type Date): JP 98196639 A 19980626

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2000020284	A	4		G06F-007/58	

Abstract (Basic): JP 2000020284 A

NOVELTY - A nonlinear conversion circuit (2) performs nonlinear conversion of the output of a linear feedback shift register (3) and a nonlinear feedback shift register (4) which operate mutually synchronizing with the same clock. A setting unit sets the initial value of both shift registers. A one-bit dummy random number is output for every one-number clock.

USE - For e.g. encryption communication apparatus.

ADVANTAGE - Estimation of initial value is made difficult.

DESCRIPTION OF DRAWING(S) - The figure is the diagram showing the basic components of the dummy random number generator. (2) Nonlinear conversion circuit; ( 3 ) Linear feedback shift register ; ( 4 ) Nonlinear feedback shift register .

Dwg.1/4

Title Terms: DUMMY; RANDOM; NUMBER; GENERATOR; ENCRYPTION; COMMUNICATE; APPARATUS; PERFORMANCE; NONLINEAR; CONVERT; OUTPUT; LINEAR; NONLINEAR; FEEDBACK; SHIFT; REGISTER; OUTPUT; ONE; BIT; DUMMY; RANDOM; NUMBER; ONE; NUMBER; CLOCK

Derwent Class: T01

International Patent Class (Main): G06F-007/58

File Segment: EPI

File 275:Gale Group Computer DB(TM) 1983-2005/May 20  
(c) 2005 The Gale Group  
File 621:Gale Group New Prod.Annou.(R) 1985-2005/May 23  
(c) 2005 The Gale Group  
File 636:Gale Group Newsletter DB(TM) 1987-2005/May 20  
(c) 2005 The Gale Group  
File 16:Gale Group PROMT(R) 1990-2005/May 20  
(c) 2005 The Gale Group  
File 160:Gale Group PROMT(R) 1972-1989  
(c) 1999 The Gale Group  
File 148:Gale Group Trade & Industry DB 1976-2005/May 23  
(c) 2005 The Gale Group  
File 624:McGraw-Hill Publications 1985-2005/May 23  
(c) 2005 McGraw-Hill Co. Inc  
File 15:ABI/Inform(R) 1971-2005/May 23  
(c) 2005 ProQuest Info&Learning  
File 647:cmp Computer Fulltext 1988-2005/May W1  
(c) 2005 CMP Media, LLC  
File 674:Computer News Fulltext 1989-2005/May W3  
(c) 2005 IDG Communications  
File 696:DIALOG Telecom. Newsletters 1995-2005/May 23  
(c) 2005 The Dialog Corp.  
File 369:New Scientist 1994-2005/Apr W2  
(c) 2005 Reed Business Information Ltd.

Set	Items	Description
S1	16058	(FEEDBACK(N)SHIFT) ()REGISTER? ? OR FSR OR SFR OR LFSR OR LSFR OR MFSR OR MSFR
S2	53	S1(5N) (DYNAMIC? OR REALTIME OR REAL()TIME OR ONDEMAND OR ON()DEMAND OR VIRTUAL?)
S3	0	(MORE() (THEN OR THAN) ()ONE) (5W) S2
S4	4	(MULTIPLE OR MULTIPLICITY OR MULTI OR SEVERAL OR MANY OR PLURAL? OR DUAL? OR VARIOUS OR NUMEROUS OR ASSORTMENT OR ADDITIONAL OR AUXILIARY OR ASSORTED OR SERIES OR ARRAY OR REDUNDANT OR SECOND? OR 2ND OR TWO OR PAIR? ? OR THREE OR 3 OR FOUR OR 4) (5N) S2
S5	228	(STATIC? OR FIXED OR PERMANENT?) (5N) S1
S6	10720	PERMUT?
S7	343577	RANDOM? OR PSEUDORANDOM?
S8	602	(KEYSTREAM OR KEY()STREAM) (3N) GENERAT? OR RNG OR PRNG
S9	0	S4(50N) S5(50N) S6
S10	0	S4(50N) S5
S11	0	S2(50N) S5
S12	1	S2(100N) S5
S13	5	S4 OR S12
S14	4	RD (unique items)

14/3,K/1 (Item 1 from file: 636)  
DIALOG(R) File 636:Gale Group Newsletter DB(TM)  
(c) 2005 The Gale Group. All rts. reserv.

05907435 Supplier Number: 123926798 (USE FORMAT 7 FOR FULLTEXT)  
More European telcos trial IPTV. (Technology)  
Screen Digest, n396, p283  
Sept, 2004  
Language: English Record Type: Fulltext  
Document Type: Newsletter; Trade  
Word Count: 228

... on a pay basis, delivering over a bandwidth of 1.5 Mbps. The service will include video-on-demand (VoD), titles costing Sfr 3 - Sfr 10 (2 (euro)-6 (euro)) per viewing, and personal video recorder (PVR) functionality. Trial customers will be...

14/3,K/2 (Item 1 from file: 16)  
DIALOG(R) File 16:Gale Group PROMT(R)  
(c) 2005 The Gale Group. All rts. reserv.

06530726 Supplier Number: 55321778  
SWITZERLAND/GERMANY: WELEDA RESULTS FOR 1998.  
Chemische Rundschau, p2  
July 2, 1999  
Language: German; NONENGLISH Record Type: Abstract  
Document Type: Magazine/Journal; Trade

ABSTRACT:  
...a slump in the pharmaceutical business. For 1998 Weleda reports a 14% fall in net profit to Sfr 4.59mn. Due to dynamic sales of body care products, turnover increased 6.1% to Sfr 170mn. The fall of profits is...

14/3,K/3 (Item 1 from file: 148)  
DIALOG(R) File 148:Gale Group Trade & Industry DB  
(c) 2005 The Gale Group. All rts. reserv.

08124425 SUPPLIER NUMBER: 17389671 (USE FORMAT 7 OR 9 FOR FULL TEXT)  
Plastics technology: manufacturing handbook & buyers' guide 1995/96. (Buyers Guide)  
Plastics Technology, v41, n8, pCOV(941)  
August, 1995  
DOCUMENT TYPE: Buyers Guide ISSN: 0032-1257 LANGUAGE: English  
RECORD TYPE: Fulltext  
WORD COUNT: 174436 LINE COUNT: 15187

... with several possible configurations. Dual fixed-spindle winders, bulk packagers (festooners), and combination winder/packagers available in several sizes. Open and closed dynamic in-line mixers and doctor-blade supply system.

Glass-roving cutters, 4 in. long to extra-wide...

14/3,K/4 (Item 2 from file: 148)  
DIALOG(R) File 148:Gale Group Trade & Industry DB  
(c) 2005 The Gale Group. All rts. reserv.

03161011 SUPPLIER NUMBER: 04775629 (USE FORMAT 7 OR 9 FOR FULL TEXT)  
Union Bank of Switzerland reports results of operations for first quarter 1987.  
PR Newswire, NYPR100  
April 24, 1987

LANGUAGE: ENGLISH        RECORD TYPE: FULLTEXT  
WORD COUNT: 460        LINE COUNT: 00044

... working capital credits or current unsecured loans increased by Sfr. 1.3 billion, mortgage loans rose by Sfr. 773 million and secured **fixed** -term loans and advances by Sfr. 496 million. Unsecured **fixed** -term loans and advances declined by Sfr. 1.6 billion (due partly to the lower dollar rate...).

... from banks remained practically unchanged at Sfr. 48.1 billion. Similarly, bills and money market paper remained virtually unchanged at Sfr. 9.5 billion.

UBS employs more than 20,000 people in more than 315 offices around the...?

29/3,K/1 (Item 1 from file: 348)  
DIALOG(R) File 348:EUROPEAN PATENTS  
(c) 2005 European Patent Office. All rts. reserv.

01021335

A method of and an apparatus for generating internal crypto-keys  
Verfahren und Vorrichtung zur Erzeugung interner Geheimschlüssel  
Procede et dispositif de generation de cles internes de chiffrage  
PATENT ASSIGNEE:

NEC CORPORATION, (236690), 7-1, Shiba 5-chome, Minato-ku, Tokyo, (JP),  
(Applicant designated States: all)

INVENTOR:

Shimada, Michio, c/o NEC Corporation, 7-1 Shiba 5-chome, Minato-ku, Tokyo  
(JP)

LEGAL REPRESENTATIVE:

VOSSIUS & PARTNER (100314), Siebertstrasse 4, 81675 München, (DE)

PATENT (CC, No, Kind, Date): EP 913964 A2 990506 (Basic)  
EP 913964 A3 020206

APPLICATION (CC, No, Date): EP 98120404 981028;

PRIORITY (CC, No, Date): JP 97314567 971031

DESIGNATED STATES: DE; FR; GB

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: H04L-009/26

ABSTRACT WORD COUNT: 133

NOTE:

Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English  
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9918	1271
SPEC A	(English)	9918	4092
Total word count - document A			5363
Total word count - document B			0
Total word count - documents A + B			5363

...SPECIFICATION way function takes comparatively long time.

Therefore, a pseudo-random-sequence generator consisting of a combination of several linear feedback-sift-registers or nonlinear feedback - shift - registers is generally used for generating the key-stream of the stream cipher, when a high speed is...

29/3,K/2 (Item 2 from file: 348)  
DIALOG(R) File 348:EUROPEAN PATENTS  
(c) 2005 European Patent Office. All rts. reserv.

00979319

Pseudorandom number sequence generator  
Pseudozufallszahlenreihengenerator  
Generateur de sequences de nombres pseudo-aleatoires

PATENT ASSIGNEE:

NEC CORPORATION, (236690), 7-1, Shiba 5-chome Minato-ku, Tokyo, (JP),  
(applicant designated states:  
AT;BE;CH;CY;DE;DK;ES;FI;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)

INVENTOR:

Shimada, Michio, NEC Corporation, 7-1, Shiba 5-chome, Minato-ku, Tokyo,  
(JP)

LEGAL REPRESENTATIVE:

Moir, Michael Christopher et al (33991), Mathys & Squire 100 Gray's Inn Road, London WC1X 8AL, (GB)

PATENT (CC, No, Kind, Date): EP 887728 A2 981230 (Basic)  
EP 887728 A3 990303

APPLICATION (CC, No, Date): EP 98304055 980521;

PRIORITY (CC, No, Date): JP 97146072 970521

DESIGNATED STATES: BE; CH; DE; FR; GB; LI  
INTERNATIONAL PATENT CLASS: G06F-007/58;  
ABSTRACT WORD COUNT: 184

LANGUAGE (Publication,Procedural,Application): English; English; English  
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9853	926
SPEC A	(English)	9853	3394
Total word count - document A			4320
Total word count - document B			0
Total word count - documents A + B			4320

...SPECIFICATION provide an explanation of a prior art nonlinear feedback shift register with reference to Figs. 1 to 3. The prior art **nonlinear feedback shift register** has an m-stage shift register 1 and a function generator which is implemented

29/3, K/3 (Item 3 from file: 348)  
DIALOG(R) File 348:EUROPEAN PATENTS  
(c) 2005 European Patent Office. All rts. reserv.

00661522  
Encryption apparatus, communication system using the same and method therefor

Verfahren und Kommunikationssystem unter Verwendung einer Verschlüsselungseinrichtung

Procede et systeme de communication utilisant un dispositif cryptographique  
PATENT ASSIGNEE:

CANON KABUSHIKI KAISHA, (542361), 30-2, 3-chome, Shimomaruko, Ohta-ku, Tokyo, (JP), (Proprietor designated states: all)

INVENTOR:

Iwamura, Keiichi, c/o Canon Kabushiki Kaisha, 30-2, 3-chome, Shimomaruko, Ohta-ku, Tokyo, (JP)

Yamamoto, Takahisa, c/o Canon Kabushiki Kaisha, 30-2, 3-chome; Shimomaruko, Ohta-ku, Tokyo, (JP)

LEGAL REPRESENTATIVE:

Beresford, Keith Denis Lewis et al (28273), BERESFORD & Co. 2-5 Warwick Court, High Holborn, London WC1R 5DH, (GB)

PATENT (CC, No, Kind, Date): EP 635956 A2 950125 (Basic)

EP 635956 A3 951206

EP 635956 B1 031022

APPLICATION (CC, No, Date): EP 94305221 940715;

PRIORITY (CC, No, Date): JP 93179232 930720; JP 93179241 930720

DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; NL; PT; SE

INTERNATIONAL PATENT CLASS: H04L-009/22

ABSTRACT WORD COUNT: 105

NOTE:

Figure number on first page: 3

LANGUAGE (Publication,Procedural,Application): English; English; English  
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200343	989
CLAIMS B	(German)	200343	875
CLAIMS B	(French)	200343	1236
SPEC B	(English)	200343	6361
Total word count - document A			0
Total word count - document B			9461
Total word count - documents A + B			9461

...SPECIFICATION known non-linear function or the DES may be used.

(Embodiment 4)

In the Embodiments 2 and 3, the linear and non-linear feedback shift registers are used to facilitate the understanding of the present invention but the essence of those embodiment resides...

29/3, K/4 (Item 4 from file: 348)  
DIALOG(R) File 348: EUROPEAN PATENTS  
(c) 2005 European Patent Office. All rts. reserv.

00565976  
Video recorder  
Videorecorder

Enregistreur video

PATENT ASSIGNEE:

MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza Kadoma, Kadoma-shi, Osaka-fu, 571, (JP), (applicant designated states: DE; FR; GB)

INVENTOR:

Hirashima, Masayoshi, 5-4-8, Kasuga Ibaraki-shi, Osaka, (JP)

LEGAL REPRESENTATIVE:

Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721), Maximilianstrasse 58, 80538 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 571753 A2 931201 (Basic)  
EP 571753 A3 940914  
EP 571753 B1 990331

APPLICATION (CC, No, Date): EP 93106242 930416;

PRIORITY (CC, No, Date): JP 92125583 920417

DESIGNATED STATES: DE; FR; GB

INTERNATIONAL PATENT CLASS: H04N-005/92; H04N-007/167;

ABSTRACT WORD COUNT: 174

LANGUAGE (Publication, Procedural, Application): English; English; English  
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9913	796
CLAIMS B	(German)	9913	702
CLAIMS B	(French)	9913	967
SPEC B	(English)	9913	8166
Total word count - document A			0
Total word count - document B			10631
Total word count - documents A + B			10631

...SPECIFICATION feedback shift register 31 shown in Fig. 3 and the sound PN generating circuit shown in Fig. 4. The nonlinear feedback shift register 31 and sound PN generating circuit 51 are each a 32-bit shift register, although a 16...

29/3, K/5 (Item 5 from file: 348)  
DIALOG(R) File 348: EUROPEAN PATENTS  
(c) 2005 European Patent Office. All rts. reserv.

00563971

A scramble codec and a television receiver incorporating the same  
Verwurfelungskodierer und Fernsehempfänger, der diesen verwendet  
Codeur de brouillage et récepteur de télévision l'utilisant

PATENT ASSIGNEE:

MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza Kadoma, Kadoma-shi, Osaka-fu, 571, (JP), (applicant designated states: DE; FR; GB)

INVENTOR:

Hirashima, Masayoshi, 5-4-8, Kasuga, Ibaraki-shi Osaka, (JP)

LEGAL REPRESENTATIVE:

Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721)

...SPECIFICATION picture signal is now described. The input picture signal, by horizontal scan line, is written in the pair of line memories and the nonlinear feedback shift register is initialized with the ID number held by said latch means to output pseudorandom pulse signals varying...

...SPECIFICATION picture signal is now described. The input picture signal, by horizontal scan line, is written in the pair of line memories and the nonlinear feedback shift register0 is initialized with the ID number held by said latch means to output pseudorandom pulse signals varying...

29/3, K/6 (Item 1 from file: 349)  
DIALOG(R) File 349: PCT FULLTEXT  
(c) 2005 WIPO/Univentio. All rts. reserv.

01204298 \*\*Image available\*\*  
A SYSTEM & METHOD FOR THE MITIGATION OF CDMA CROSS-CORRELATION ARTIFACTS  
AND THE IMPROVEMENT OF SIGNAL-TO-NOISE RATIOS IN TDMA LOCATION NETWORKS  
SYSTEME ET PROCEDE D'ATTENUATION DES ARTEFACTS DE CORRELATION CROISEE AMCR  
ET AMELIORATION DES RAPPORTS SIGNAL SUR BRUIT DANS LES RESEAUX DE  
LOCALISATION AMRT

Patent Applicant/Assignee:

LOCATA CORPORATION, 9 Island View, Irvine, CA 92604, US, US (Residence),  
US (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:

LAMANCE James, 2000 Wisteria Drive, Hixon, TN 37343, US, US (Residence),  
US (Nationality), (Designated only for: US)

SMALL David, Unit 6

(Residence), AU (Nationality), (Designated only for: US)  
Legal Representative:

SMALL David (commercial rep.), 401 Clunies Ross St, AC

Patent and Priority Information (Country, Number, Date):

Patent: WO 200513633 A1 20050210 (WO 0513633)

Application: WO 2004AU1025 20040803

### Priority Application

Designated States:  
(All protection types applied unless otherwise stated - for applications

04+)  
 AE AG AL AM AT AU AZ BA BB BG BR BW BY BZ CA CH CN CO CR CU CZ DE DK DM  
 DZ EC EE EG ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC  
 LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NA NI NO NZ OM PG PH PL PT RO  
 RU SC SD SE SG SK SL SY TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW

(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PL PT RO  
SE SI SK TR  
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG  
(AP) BW GH GM KE LS MW MZ NA SD SL SZ TZ UG ZM ZW  
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 10226

Fulltext Availability:

Detailed Description

Detailed Description

... of a simplified position receiver channel illustrating a TDMA correlator engine, according to the present invention, further incorporating a PRN Preset Selector, a PRN Track Selector, and two PRN Code Generators.

#### I 0 OVERVIEW

A plurality of...the TDMA correlator engine. A traditional receiver generates the PRN codes that determine the code phase in real time with a series of linear feedback shift registers (LFSR). To change the code phase, the linear feedback shift registers (LFSR) are advanced or held constant providing a relative code phase change with respect to the incoming broadcast signal. With TDW positioning signals, slewing the code phase generated by a linear feedback shift register (LFSR) to the correct phase for each programmed integration interval is not possible because the time required to...

29/3,K/7 (Item 2 from file: 349)  
DIALOG(R) File 349:PCT FULLTEXT  
(c) 2005 WIPO/Univentio. All rts. reserv.

00917574 \*\*Image available\*\*

METHOD AND SYSTEM FOR TRUSTED DIGITAL CAMERA  
PROCEDE ET SYSTEME D'APPAREIL PHOTOGRAPHIQUE VALIDE

Patent Applicant/Assignee:

APPLIED SCIENCE FICTION, 8980 Business Park Drive, Austin, TX 78759, US,  
US (Residence), US (Nationality)

Inventor(s):

HAMILTON Jon W, 2502 Rural Route 1323, Johnson City, TX 78636, US,

Legal Representative:

TALPIS Matthew B (agent), Baker Botts LLP, Suite 600, 2001 Ross Avenue,  
Dallas, TX 75201-2980, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200251126 A2-A3 20020627 (WO 0251126)

Application: WO 2001US50271 20011221 (PCT/WO US0150271)

Priority Application: US 2000257918 20001221

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AT (utility model) AU AZ BA BB BG BR BY BZ CA CH CN CO CR  
CU CZ CZ (utility model) DE DE (utility model) DK DK (utility model) DM  
DZ EC EE EE (utility model) ES FI FI (utility model) GB GD GE GH GM HR HU  
ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX  
MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SK (utility model) SL TJ TM TN  
TR TT TZ UA UG UZ VN YU ZA ZW  
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR  
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG  
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW  
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 17390

Fulltext Availability:  
Detailed Description  
Claims

Detailed Description

... of both

randomness and smoothness: (1) number of rounds f or SI;  
(2) maximum number of twiddles; (3) specific design for  
non-linear feedback shift register #3; (4) specific  
design for non-linear feedback shift...  
... nibble when nibble test succeeds; and (8)  
specific design for the rotation matrix. For example,  
non-linear feedback shift register #4 may be designed  
based on non-linear feedback shift registers number one,  
two and three, or may use another suitable design.

In the SI box, incoming blocks of cipher data are  
sent forth through non-linear feedback shift register 43  
(see FIGURE 29) and then through the twiddle loop for a  
predetermined and constant number of...

Claim

... The method according to Claim 49, wherein  
applying the first S box comprises:  
applying a first non-linear feedback shift register  
to the partition;  
selecting a nibble from the partition;  
comparing the selected nibble against...been applied to the partition.

55 The method according to Claim 54, wherein the  
-first non-linear feedback shift register comprises a non  
linear feedback shift register number three and the  
second non-linear feedback shift register comprises a  
non-linear feedback shift register number four.

56 The method according to Claim 49, wherein the  
second S box comprises:  
determining a...

...comprises:  
applying a rotation matrix to at least one of the  
nibbles in the partition  
applying a second nonlinear feedback shift register  
to the partition  
selecting a nibble from the partition;  
comparing the selected nibble...

...feedback shift register  
to the partition.

60 The method according to Claim 59, wherein the  
first non-linear feedback shift register comprises a non  
linear feedback shift register number three and the  
second non-linear feedback shift register comprises a  
non-linear feedback shift register number four.

61 The method according to Claim 57, wherein  
applying the reverse P box comprises:  
rotating...

...The system according to Claim 63, wherein the  
software is further operable to:  
apply a first non-linear feedback shift register to  
the partition;

select a nibble from the partition;  
compare the selected nibble against...

...been applied to the partition.

69 The system according to Claim 68, wherein the first non-linear feedback shift register comprises a non linear feedback shift register number three and the second non- linear feedback shift register comprises a non- linear feedback shift register number four.

70. The system according to Claim 63, wherein the software is further operable to...comprises:  
applying a rotation matrix to at least one of the nibbles in the partition

applying a second nonlinear feedback shift register to the partition  
selecting a nibble from the partition;

comparing the selected nibble against an entry in...

..shift register  
5 to the partition.

74 The method according to Claim 73, wherein the first non- linear feedback shift register comprises a non linear feedback shift register number three and the second non- linear feedback shift register comprises a non- linear feedback shift register number four.

75 The method according to Claim 71, wherein applying the reverse P box comprises:  
rotating...

29/3,K/8 (Item 3 from file: 349)  
DIALOG(R) File 349:PCT FULLTEXT  
(c) 2005 WIPO/Univentio. All rts. reserv.

00815044 \*\*Image available\*\*  
COMPUTER EFFICIENT LINEAR FEEDBACK SHIFT REGISTER  
REGISTRE INFORMATIQUE A DECALAGE A REBOUCLAGE LINEAIRE  
Patent Applicant/Assignee:

HONEYWELL INC, 101 Columbia Avenue, P.O. Box 2245, Morristown, NJ 07960,  
US, US (Residence), US (Nationality)

Inventor(s):

DRISCOLL Kevin, 7249 West Timber Lane, Maple Grove, MN 55369, US,

Legal Representative:

HOIRIIS David (et al) (agent), Honeywell Inc., 101 Columbia Avenue, P.O.  
Box 2245, Morristown, NJ 07960, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200148594 A2-A3 20010705 (WO 0148594)

Application: WO 2000US32633 20001201 (PCT/WO US0032633)

Priority Application: US 99453008 19991202

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB  
GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA  
MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA  
UG UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 5888

Fulltext Availability:  
Detailed Description

Detailed Description  
... by the cryptanalyst.

The non-linearization techniques include "clock control" (the LFSRs are advanced pseudo-randomly), non-linear transforms of the LFSR output, and non-linear combination of multiple LFSR. Any or all of these means can be used with the present invention. In Figure 2, optional post processor 110 can be employed to perform post processing, such as non-linear filtering, of the LFSR 100 output to non-linearize the LFSR output to prevent certain plaintext attacks. In the embodiment illustrated...